UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/031,291	01/14/2002	Takayuki Nakajima	9683/100	2536

7590 01/25/2005

Brinks Hofer Gilson & Lione
P O Box 10395
Chicago, IL 60610

EXAMINER	
BADII, BEHRANG	
ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 01/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/031,291	**Applicant(s)** NAKAJIMA ET AL.	
	Examiner Behrang Badii	**Art Unit** 3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 January 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 January 2002* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *7/26/04*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claims 1-23 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vatanen, U.S. patent 6,169,890, and further in view of Vilander et al., U.S. patent 6,553,219.

As per claim 1, Vatanen discloses an authentication system (abstract, Fig. 3) comprising:

a plurality of receiving 'terminals for receiving a transaction request from a user (col.4, lines 8-38);

a mobile communication network for serving a plurality of mobile communication terminals (col.2, lines 58-65);

Vatanan does not disclose a first location memory storage device for storing a location of each of said plurality of terminals;

a second location memory storage device for storing a location of each of said plurality of mobile communication terminals;

a matching device for obtaining from said first location memory storage device a location of a receiving terminal which has received transaction request, and for obtaining from said second location

memory storage device a location of a mobile communication terminal, transmitting the transaction request, and matching each of said locations; and

an authentication device for determining a validity of said transaction request based upon a result obtained by said matching device upon comparing said locations.

Vilander et al. discloses a first location memory storage device (database, register) for storing a location of each of said plurality of terminals (Fig.1 and 3; col.1, 29-47; col.5, 15-43);

a second location memory storage device for storing a location of each of said plurality of mobile communication terminals (Fig.1 and 3; col.1, 29-47; col.5, 15-43);

a matching device for obtaining from said first location memory storage device a location of a receiving terminal which has received transaction request, and for obtaining from said second location

memory storage device a location of a mobile communication terminal, transmitting the transaction request, and matching each of said locations (col.2, 35-53; col.3, 43-60; col.5, 15-43); and

an authentication device for determining a validity of said transaction request based upon a result obtained by said matching device upon comparing said locations (col.2, 35-53; col.3, 43-60; col.5, 15-43).

It would have been obvious to modify Vatanen to include a first location memory storage device for storing a location of each of said plurality of terminals;

a second location memory storage device for storing a location of each of said plurality of mobile communication terminals;

a matching device for obtaining from said first location memory storage device a location of a receiving terminal which has received transaction request, and for obtaining from said second location

memory storage device a location of a mobile communication terminal, transmitting the transaction request, and matching each of said locations; and

an authentication device for determining a validity of said transaction request based upon a result obtained by said matching device upon comparing said locations such as that taught by Vilander et al. in order to secure the transaction such that the correct user can carry out the transaction based upon the matching and authentication of the location of the mobile object and the receiving terminal.

As per claim 2, Vatanen further discloses a mobile communication terminal carried by the user who has transmitted said transaction request is identified by identification information contained in said transaction request (col.1, lines 61-67; col.2, lines 1-4).

As per claim 3, Vatanen further discloses a cellular network including a plurality of base stations; and said second location storing device obtains a location of said mobile communication terminal by detecting a base station located near said mobile communication terminal (Fig.2; col.4, lines 8-38).

As per claim 4, Vilander et al. further discloses obtaining a location based upon radio waves transmitted from a satellite (Fig.1; col.3, lines 17-26; col.4, lines 5-32).

As per claim 5, Vatanen further discloses obtaining operation of a location of said mobile communication terminal by said second location storing device is initiated when said user operates said mobile communication terminal (Fig.2; col.4, lines 8-38).

As per claim 6, Vatanen further discloses receiving terminal is a communication terminal served by another communication network connected to said mobile communication network (abstract; Fig.3); and

wherein, while said matching device is installed in said mobile communication network, said authentication device is installed in said another communication network (Vilander et al, col.5, lines 15-43) and (Vatanen, col.3, lines 8-14).

As per claim 7, Vatanen further discloses receiving terminal is a second mobile communication terminal served by said mobile communication network (abstract, Fig.3); and wherein said first location storing device obtains a location of said receiving terminal for storage by detecting a base station located near said receiving terminal (Fig.2; col.4, lines 8-38).

As per claim 8, Vatanen further discloses receiving terminal is a second mobile communication terminal served by said mobile communication network (Fig.2; abstract; col.3, lines 56-67; col.4, lines 1-38); and

Vilander et al further discloses wherein said first location storing device obtains a location of said receiving terminal for storage based upon radio waves transmitted from a satellite (col.3, lines 17-26; col.4, lines 5-32).

As per claim 9 Vatanen further discloses an authentication system (Vatanen, Fig.3, abstract) comprising:

a plurality of receiving terminals for receiving a transaction request by reading, from an identification card (col.1, lines 61-67; col.2, lines 1-4) storing identification information of a user, identification information of the user (col.4, lines 8-38);

Vilander et al. further discloses a first location storing device for storing location information of each receiving terminal and identification information of each of said receiving terminals as corresponding to each other (Fig. 1 and 3; col.1, lines 29-47; col.5, lines 15-43);

a second location storing device for storing location information of a mobile communication terminal of each user and identification information of each of said user as corresponding to each other (Fig.1 and 3; col.1, lines 29-47; col.5, lines 15-43);

a matching device for matching location information of said receiving terminal with location information of a mobile, communication terminal, location information of said receiving terminal being read out as a key which is identification information of an receiving terminal which received said transaction request from said first location memory device read out as a key which is identification information of a user who transmitted said transaction request from said second location memory device (col.2, lines 35-53; col.3, lines 43-60; col.5, lines 15-43);

an authentication device for determining authenticity of said user based upon a match result by said matching device (col.2, lines 35-53; col.3, lines 43-60; col.5, lines 15-43).

As per claim 10, Vatanen and Vilander et al. further disclose a database for retaining amount data indicating an amount available for said user in correspondence with said identification information regarding said user (Vatanen: col.4, 8-38; col.6, 46-51; claim 8);

wherein while said mobile communication terminal comprises a memory for storing the identification information regarding said user and a first communication interface for performing communication with said receiving terminal, said receiving terminal comprises a second communication interface for performing radio communication with said first communication interface of said mobile communication terminal (Vilander et al: col.3, 17-26; col.4, 5-32);

said mobile communication terminal transmits said identification information read out from said memory via said first communication interface (Vilander et al: Fig.2; abstract; col.2, 35-53; col.3, 43-60);

said receiving terminal receives said identification information via said second communication interface and transmits it to said authentication device (Vilander et al: Fig.2; abstract; col.2, 35-53; col.3, 43-60);

said authentication device determines authenticity of said user by referring to a transaction amount required for said transaction request and amount data stored in said database (Vatanen: col.4, 8-38; col.6, 46-51; claim 8) in correspondence with said received identification information in addition to a match result given by said matching device (Vilander et al: col.2, lines 35-53; col.3, lines 43-60; col.5, lines 15-43).

As per claim 11, Vatanen and Vilander et al. further disclose a mobile communication terminal storing amount data denoting an amount available for said user (Vatanen: col.4, 8-38; col.6, 46-51; claim 8) and transmits it together with said identification information read out from said memory via said first communication interface (Vilander et al: Fig.2; abstract; col.2, 35-53; col.3, 43-60); and

said receiving terminal determines authenticity (Vilander et al: col.2, lines 35-53; col.3, lines 43-60; col.5, lines 15-43) of said user by referring to a transaction amount required for said transaction request and said amount data transmitted from said mobile communication terminal (Vatanen: col.4, 8-38; col.6, 46-51; claim 8).

As per claim 12, Vilander et al. further discloses first communication interface and said second communication interface perform radio communication (Fig.1; col.3, 17-26; col.4, 5-32).

As per claim 13 and 14, Vatanen further discloses that the mobile communication terminal is a cellular telephone (title and abstract).

As per claim 15, Vatanen further discloses an authentication method (Fig.; abstract) for determining authenticity of a user who possesses a mobile communication terminal served in a mobile communication network (Fig.3; col.2, 58-65), the method comprising:

a step of receiving a transaction request from a user at each receiving terminal (col.4, 8-38);

Vilander et al, further discloses a first location finding step for finding a location of an receiving terminal which has received said transaction request (Fig. 1 and 3; col.1, lines 29-47; col.5, lines 15-43);

a second location finding step for finding a location of a mobile communication terminal which should be possessed by a user who transmitted said transaction request (Fig. 1 and 3; col.1, lines 29-47; col.5, lines 15-43);

a step for matching the location of said receiving terminal found by said first location finding step with the location of said mobile communication terminal found by said second location finding step (col.2, lines 35-53; col.3, lines 43-60; col.5, lines 15-43); and a step for determining authenticity of a transaction request based upon a result given by said matching step (col.2, lines 35-53; col.3, lines 43-60; col.5, lines 15-43).

As per claim 16, Vatanen further discloses a mobile communication terminal possessed by a user who transmits said transaction request is identified by identification information contained in said transaction request (col.1, 61-67; col.2, 1-4).

As per claim 17, Vatanen further discloses a cellular network in which a plurality of base stations are placed (title and abstract); and

said second location finding step finds a location of said 30 mobile communication terminal by detecting said mobile station located near said mobile communication terminal (Fig.2; col.4, 8-38).

As per claim 18, Vilander et al. further discloses receiving an operation to request a location detection of said mobile communication terminal by said user at said mobile communication terminal;

wherein said step for finding a location of said mobile communication terminal is initiated by reception of said operation (col.4, 66-67; col.5, 1-15).

As per claim 19, Vatanen and Vilander et al. further disclose an authentication method for determining authenticity of a user who possesses a mobile communication terminal served in a mobile communication network (Vatanen: Fig.3, abstract), comprising:

a stepof receiving a transaction request at each receiving terminal (Vatanen: col.4, lines 8-38) by reading out identification information of this user from an ID card in which identification information of a user is stored (Vatanen: col.1, 61-67; col.2, 1-4);

a step of reading out location information (Vilander et al.: col.1, 29-47) of this receiving terminal based upon a key (Vatanen: col.4, 8-38) which is identification information of an receiving terminal which has received said transaction request from data which identification information of each receiving terminal has stored in relation to location information of said each receiving terminal beforehand (Vilander et al: Fig.1 and 3; col.1, 29-47; col.5, 15-43);

a step of reading out location information of a mobile communication terminal which this user should possess based upon a key (Vatanen: col.4, 8-38) which is identification information of a user who has transmitted said transaction request from data in which identification information of each user has been stored in relation to location information of a mobile communication terminal beforehand (Vilander et al: Fig.1 and 3; col.1, 29-47; col.5, 15-43);

a step of matching said location information of receiving terminal which was read out with said location information of a mobile communication terminal which was read out (Vilander et al.: col.2, 35-53; col.3, 43-60; col.5, 15-43);

an authentication step of determining authenticity of said user based upon a result of said match (Vilander et al.: col.2, 35-53; col.3, 43-60; col.5, 15-43).

As per claim 20, Vatanan and Vilander et al. further disclose a step of storing amount data indicating an amount available for said user in correspondence with said identification information on said user beforehand (Vatanen: col.4, 8-38; col.6, 46-51; claim 8);

a step of transmitting in which said mobile communication terminal transmits identification information regarding said user to 5 said receiving terminal (Vilander et al: Fig.2; abstract; col.2, 35-53; col.3, 43-60);

a step of receiving in which said receiving terminal receives said identification information which was transmitted (Vilander et al: Fig.2; abstract; col.2, 35-53; col.3, 43-60); and

wherein said authentication step determines authenticity of said user by referring to a transaction amount required for said transaction request and said amount data which is stored (Vatanen: col.4, 8-38; col.6, 46-51; claim 8) in correspondence with said identification information received by said receiving terminal in addition to said match result (Vilander et al.: col.2, 35-53; col.3, 43-60; col.5, 15-43).

As per claim 21, Vatanen further discloses an authentication program (Fig.3, abstract) for determining authenticity of transaction request by a user who possesses a mobile communication terminal served in a mobile communication network wherein a computer prompts the program to execute (Fig.3, col. 2, 58-65);

Vilander et al. further discloses a first process of location finding for finding a location of said each receiving terminal which has received said transaction request when each receiving terminal has received a transaction request of a user (Fig.1 and 3; col.1, 29-47; col.5, 15-43);

a second location finding process for finding a location of a mobile communication terminal which a user who transmitted said transaction request should possess (Fig.1 and 3; col.1, 29-47; col.5, 15-43);

a match process for matching a location of said receiving terminal which was found by said first location finding process with a location of said mobile communication terminal found by said second location finding process (col.2, 35-53; col.3, 43-60; col.5, 15-43); and

an authentication process for determining authenticity of said user based upon said match result (col.2, 35-53; col.3, 43-60; col.5, 15-43).

As per claim 22, Vatanen and Vilander et al. further disclose an authentication program (Vatanen: Fig.3, abstract) for determining authenticity of transaction by a user who possesses a mobile communication terminal served in a mobile communication network wherein a computer prompts the program to execute (Vatanen: Fig.3; col.2, 58-65);

a process of reading out location information (Vilander et al.: Fig.1 and 3; col.1, 29-47; col.5, 15-43) of this receiving terminal based upon a key (Vatanen: Col.4, 8-38) which is identification information of an receiving terminal which has received said transaction request from data in which identification information of said each receiving terminal has been stored in correspondence with location information of said each receiving terminal beforehand when identification information of said each receiving terminal and said user have been obtained after each receiving terminal has received a transaction request from a user (Vilander et al.: Fig.1 and 3; col.1, 29-47; col.5, 15-43);

a process of reading out location information (Vilander et al.: Fig.1 and 3; col.1, 29-47; col.5, 15-43) of a mobile communication terminal which this user should possess based upon a key (Vatanen: Col.4, 8-38) which is identification information of a user who transmitted said transaction request from data in which identification information of each user has been stored in correspondence with location information of a mobile communication terminal beforehand (Vilander et al.: Fig.1 and 3; col.1, 29-47; col.5, 15-43);

a process for matching said location information of receiving terminal which was read out with said location information of a mobile communication-terminal which was read out (Vilander et al.: col.2, 35-53; col.3, 43-60; col.5, 15-43);

authentication process for determining authenticity of said user based upon said match result (Vilander et al.: col.2, 35-53; col.3, 43-60; col.5, 15-43).

As per claim 23, Vatanen et al. further discloses a computer-readable recording media storing the program (abstract, Fig.1).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ketcham (U.S. patent 6,075,860) discloses an apparatus and method for authentication and encryption of a remote terminal over a wireless link.

Ahvenainen (U.S. patent 6,199,161) discloses a management of authentication keys in a mobile communication system.

Ownens et al. (U.S. patent 6,338,140) discloses a method and system for validating subscriber identities in a communications network.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Behrang Badii whose telephone number is 703-305-0530. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 703-305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

Behrang Badii
Patent Examiner
Art Unit 3621

BB